The U.S. Air Force's Cryptologic Systems Group: Putting the "Super" in Information Superiority

By

Gregory L. Garcia
Electronic Systems Center

Introduction

Based on the dramatic shifts in both political and military dimensions coupled with today's rapid technical advancements, there is clear impetus to reexamine the elements of an effective military strategy. The struggle is no longer limited to known protagonists surveying the field to monitor, assess, and counter an identified antagonist. The focus of warfare, with its past heavy reliance on kinetic weapons, such as bombs, missiles, and bullets, has widened to include the burgeoning requirement to fight the daily struggle of the non-kinetic world, the fight for information and the counter force of information assurance, the struggle for information superiority. In the midst of this battle, the Cryptologic Systems Group, a geographically separated unit of the Electronic System Center within the Air Force Materiel Command, hones people, systems, and knowledge to enable both the Air Force and international partners to garner information while assuring the protection of their critical data.

Place in the Changing Milieu

The conventional approach of understanding the tenets of non-kinetic warfare is to divide activities into the broad category of information operations (IO) with partitions for information-in-warfare (IIW) and information warfare (IW).[1] This schema identifies a subcategory of activities to achieve the four IO objectives of gain, exploit, attack and defend critical capabilities in this evolving non-kinetic environment. Few nation-states or rogue actors are positioned to coordinate a broad attack across the U.S. or North Atlantic Treaty Organization countries. Rather, these potential adversaries seek the same advancement of IIW or IW to gain, exploit, or attack established governments' infrastructure or individuals as exhibited in the exponential increase in hostile computer probes and intrusions. These incidents focus on political and financial as well as military targets.

These operations resonate across the global information grid undetected or masked. Many times organizations specifically designed to monitor such events, like the U.S. National Infrastructure Protection Center, are undermanned and unable to coalesce useful and timely warnings.[2] With the growing use of these global information communication mechanisms, such as the world wide web or public phone services, and the increased use of network information systems for mission data, the threat of increased non-kinetic attacks is predictable.

For those with national security responsibilities, attention must be afforded to the crucial daily struggle of turning data into information and then securing those rudiments. Understanding, preparing, and winning this non-kinetic war is a prerequisite for achieving information superiority. For the CPSG, it is our mission to equip selected combatants with the necessary tools, systems, and training to ensure they are able to obtain information superiority to dominate both the kinetic and non-kinetic battlefields.

CPSG Organization

The CPSG mission is to directly support the warfighters' secure command, control, and intelligence exigencies. This applies to active U.S. Air Force, NATO members, and international partnerships.[3] The CPSG provides cryptologic sustainment for keying material, item management, storage, shipment, and joint-service depot-level hardware and trusted software maintenance for information assurance, intelligence, force protection and other related systems. CPSG is the Information Assurance Product Area Directorate and the Air Force system program office for public key infrastructure with direct links to Headquarters United States Air Force and Defense Information Infrastructure. CPSG manages special compartmental projects for the Department of Defense and National Security Agency space systems. CPSG provides the engineering, logistics support and maintenance functions for the Air Force Technical Applications Center's material collection systems that support the United States Atomic Energy detection system. Additionally, CPSG is the joint-service, consolidated signal intelligence support activity that manages over 1,000 such systems.

Protecting the Infrastructure

Research
- VARM
- Lighthouse
- Biometrics

Programs
- PKI
- CAC

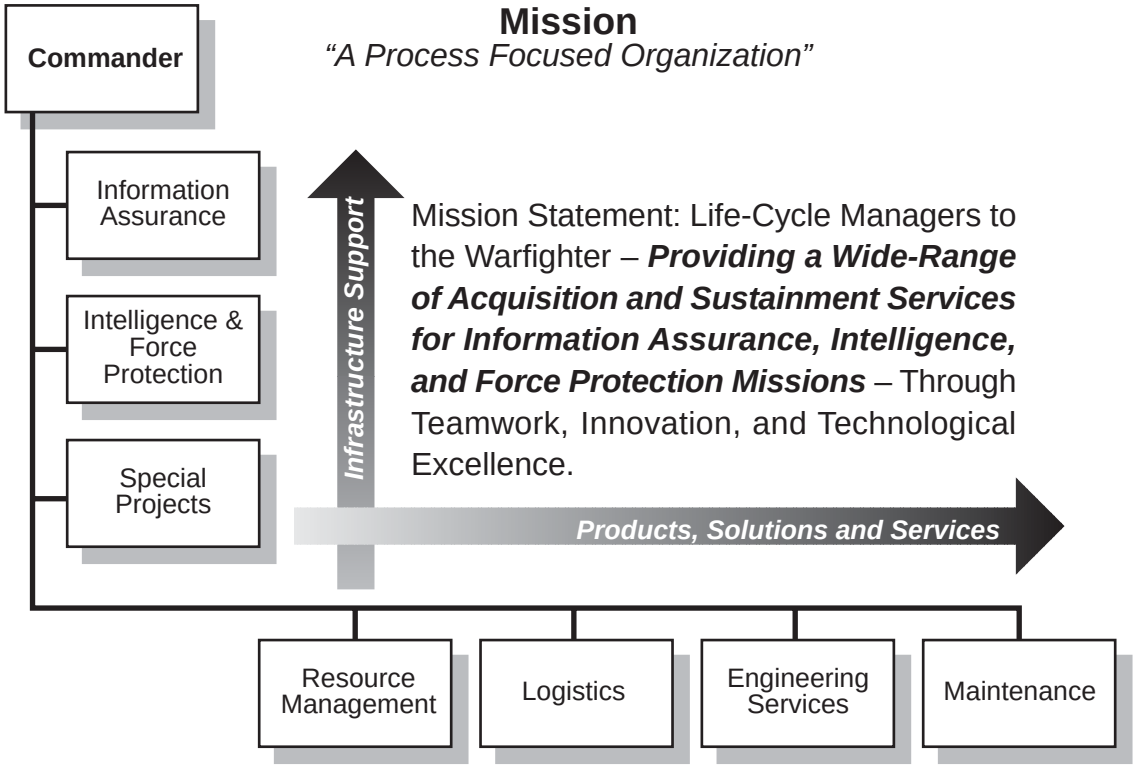
Infrastructure
- E-Crypto
- ITAC
- NAL

Support to Both the War-Fighter and Infrastructure

With a view to front line war-fighters, CPSG is involved in performing and securing the information needed to perform their assigned missions. At the base level, CPSG supports systems that protect the base physical boundary and weapon system storage facilities. The air planning is conducted with information from intelligence systems maintained by CPSG. The voice call sign designations and secure communication devices for voice, data, and navigational data for Air Force and some international partners are systems managed, repaired, and delivered by our organization.

In the area of signal intelligence support, CPSG established one of the most responsive repair and return programs throughout the Department of Defense. Through an integrated product team approach, the organization has established a web-based status system to provide the latest information on the status of each particular requirement. The team has streamlined the process of receipt, maintenance, and return within a robust management structure. The end result of this initiative is a competent and effective source of supply across a broad range of systems, components and projects. Additionally, on the information assurance side, CPSG is fielding a unique "e-crypto" e-business initiative that will allow select customers to forward requirements,

purchase orders, repair actions, and ask technical questions all in an electronic environment. This initiative is expected to reduce lead-times, lower prices, and increase customer service for Air Force and international partners.



Additionally, CPSG is working to secure the infrastructure where much of this critical information travels, both for classified and unclassified data. As the Air Force implementer of the public key infrastructure, CPSG will touch every Air Force member in providing a secure token that will enable each individual to sign and encrypt all unclassified e-mail traffic ensuring identity, authentication, confidentiality, integrity, and proof of participation. Moreover, the group is working on the forthcoming deployment of a smart card implementation of the Department of Defense common access card efforts. This card will serve as the new means of identification for all service members, the token for signing and encrypting e-mail, and a host of future applications. CPSG recently was designated as the Air Force program office for biometrics research and integration planning initiatives within the Air Force.

CPSG also excels in the area of engineering and research. A capability we provide is our Information Assurance Technical Assistance Center (ITAC). This group of individuals provides world-class engineering and technical assistance across the full spectrum of secure issues. They also serve as a node on the ESC network applications lab, which provides a means of rapidly prototyping emerging and critical information warfare ideas, techniques and advancements. Additionally, CPSG manages two research programs: cyber lighthouse and vulnerabilities assessment and risk management. These efforts assist in development and proofing of systems designated for implementation. Based on technology assessment, our efforts are built around filling the gap of documented mission needs and systems to provide that specific capability.

Support to International Partners

We pride ourselves in our unparalleled support to our international partners. Both in the information-in-warfare and information warfare arenas, our organization provides equipment and system support in meeting our partners' national security needs. The following list depicts a brief synopsis of key programs that we currently support:

- United Kingdom C-17 logistic support program
- Australian airborne early warning and control (AEW&C) project.
- KOK-22 and 22A maintenance and rectification support program
- Israel; PEACE MARBLE V system sale (F-16)
- Israel; F-15I Air Force program
- Korean; F-15 Fighter program
- NATO AWACS E-3A program
- Maintenance repair and return support to NATO countries and other allied countries for IA equipment and systems
- Technical support on development of letters of offers for countries regarding system sales considerations

The Super in Information Superiority

The challenge of the non-kinetic battlefield is to remain vigilant, active, and equipped. By no means does CPSG work as the sole provider or without coordination of other organizations. Information organizations within this environment is a congeries of supporting participants. It is in this strength of a multi-entity approach, an interconnected net of partners, in which information organizations can succeed in ferreting out those ill intentions of others versus the chatter and clamor of a bustling world. It is in obtaining information superiority, based on the information-in-warfare and information warfare tenets, that these assaults on our information domains can be halted and defused. Within this environment, CPSG stands ready to serve the needs of those faced with the responsiblity of protecting their countries as life cycle managers to the war-fighter putting the super in information superiority.

About the Author

Gregory L. Garcia is the acting director of the Information Assurance Product Area Directorate, Electronic Systems Center, United States Air Force, located at the Cryptologic Systems Group in San Antonio Texas. He has sixteen years of U.S. government experience and holds a master degree's in public policy from the Woodrow Wilson School of Public and International Affairs, Princeton University and a master's degree in business administration from University of the Incarnate Word, San Antonio Texas.

End Notes

1 *Air Force Doctrine Document* 2-5, 5 August 1998, page 3.

2 GAO Report, GAO-01-323, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, 25 April 2001.

3 Larry Kisher and Harold Stamler, CPSG Mission Brief/Organization Summary, May 01.